Quantifying and managing the risk of information security breaches to the supply chain

by

Cynthia Lynn Bellefeuille

AB
Dartmouth College

Submitted to the Engineering Systems Division in Partial Fulfillment of the Requirements for the Degree of

Master of Engineering in Logistics

at the

Massachusetts Institute of Technology

June 2005

Signature of Author .....
Engineering Systems Division

Certified by .....
George Kocur
Senior Lecturer
Thesis Supervisor

Accepted by .....
Yossi Sheffi
Professor of Civil and Environmental Engineering
Professor of Engineering Systems
Director, MIT Center for Transportation and Logistics

BARKER

Quantifying and managing the risk of information security breaches to the supply chain

By

Cynthia Lynn Bellefeuille

Submitted to the Engineering Systems Division

On 6 May 2005 in Partial Fulfillment of the

Requirements for the Degree of Master of Engineering in Logistics

Abstract

Technical integration between companies can result in an increased risk of information security breaches. This thesis proposes a methodology for quantifying information security risk to a supply chain participant. Given a system responsible for supply chain interaction and the vulnerabilities attributed to the system, the variables that determine the probability and severity of security incidents were used to create a model to quantify the risk within three hypothetical information systems. The probability of an incident occurring was determined by rating the availability and ease of performing an exploit, the attractiveness of the target and an estimate of the frequency of the attack occurring internet wide. In assigning a monetary value to the incident, the outcome from an attack was considered in terms of the direct impact on the business process and the potential impact on partnerships. A method for determining mitigation strategies was then proposed based on a given set of monetary constraints and the realization of corporate security policy.

Thesis Supervisor: George Kocur
Title: Senior Lecturer, Department of Civil and Environmental Engineering, Massachusetts Institute of Technology, Cambridge, Massachusetts.

Acknowledgements

Firstly, I would like to thank my advisor, Dr. George Kocur. His generous support, guidance, and kind manner made this thesis experience enjoyable. Dr. Chris Caplice for his dedication to the improvement of the MLOG program and in turn his commitment to all MLOG students.

I would like to thank my colleagues at NetSec for their encouragement and assistance with my project. The ideas and advice that were so generously shared by Martyn Ruks and Tom Parker were greatly appreciated. I would like to thank Jack Whitsett for his generous gift of time to help me gather data and tirelessly offer me guidance. I would also like to acknowledge Glenn Hazard for his endorsement of my time at MLOG, and David Howorth for always being ready to offer kind words, suggestions and support.

Finally, I would like to thank my parents for their boundless support and encouragement beginning at my first breath. Without their impassioned belief in the value of education and hard work, I would not be where I am today. Spending this year with my sister and parents in Boston, after many years away from home, has been a real pleasure.

Table of Contents

List of Figures

List of Tables

List of Equations

1 Introduction

Efficiencies and improvements in supply chain interactions have been achieved through the use of technology to support information transfer and collaboration. The electronic tools that have delivered these benefits to companies' supply chains may present potential risk to both the reputation and financial standing of the beneficiary companies, as a result of information security breaches. As companies that have benefited from sharing information are aware, the value of information is often considered to be at least as important as the value of physical assets. Protecting the confidentiality, integrity, accuracy and accessibility of company information is important to a firm's ability to function in today's supply chains.

Understanding the risk that information security breaches can pose to the supply chain is important not only in for an operational perspective, but in order to comply with regulations such as Sarbanes Oxley Act of 2002. Further any company that holds individual customer data must comply to standards for the protection of that data though laws such as the California Security Breach Information Act, Senate Bill 1386 of 2002 or in the case of the healthcare industry, patient data as regulated by Health Insurance Portability and Accountability Act of 1996 (HIPAA). The expectation of maintaining the security of other company's data may also be specified in procurement or partnership contracts.

This thesis will describe a methodology for performing a quantitative risk assessment on three partners in a supply chain. This assessment will be comprised of an asset identification phase, a

vulnerability assessment phase, an outcome identification phase and finally the calculation of expected loss phase. Once the expected value of loss has been determined, mitigation plans to address four different company objectives, minimizing expected value of loss, loss of availability, loss of information integrity and information disclosure, are proposed.

2 Motivation

Several studies have concluded companies can greatly improve their supply chain performance through online collaboration. Kapucinski, Zhang, Carbonneau, Moore and Reeves (2004) found that Dell could obtain $43 million in potential annual savings through "e-commerce and manufacturing initiatives" aimed at lowering inventory held by their suppliers at Dell manufacturing facilities. Savings of this magnitude are certainly in the best interest of companies, but the risk that online collaboration may pose to a company must also be considered so that the necessary mitigation strategies can be put in place.

As online collaboration within the supply chain increases, the potential consequence of an attack resulting in a loss of availability, loss of data integrity or unauthorized disclosure of information also increases. The SCOR model identifies five supply chain management processes: source, deliver, make, plan and return (Huan, S, Sheoran, S, Wang, G., (2004). There are commercially available and internally developed software applications that have been developed to facilitate these processes. The prospect of one or more of these functions being crippled due to an application being unavailable could result in financial losses for the company. Further, the inability to service customers during that unavailability could impact a company's reputation and customer relationships, possibly resulting in customers ceasing to trade with the affected company.

A company's assets are now being considered as not only the physical inventory, property and staff of the firm, but also as the information that the company possesses. Information security breaches resulting in a loss of data integrity or the disclosure of sensitive information to other unwanted parties are another potential risk to a company's financial position. Supply chain collaboration activities require the exchange of data, much of it sensitive, with trusted partners. A breach of a company's information systems could result in the disclosure not only of its information, but also its trading partners' sensitive data. Typically collaboration is practiced with a company's most critical trading partners. Potentially losing a trading partner as a result of data corruption would have a negative impact on a company.

Compliance with regulations is also making the need to evaluate information security within firms a priority. The introduction of the Sarbanes Oxley Act of 2002 (SOX) has made it imperative for companies to recognize, quantify and manage risks within a corporation. The section of SOX that is of particular relevance to supply chain related information security concerns is section 404. This section requires an internal controls report which should include the following: "a statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company; management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year; a statement identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting; and a statement that the registered public accounting firm that audited the company's financial statements included in the annual report has issued an attestation report on management's assessment of the company's internal control over financial reporting" (Sarbanes Oxley Act of

2002). The obvious result of the reporting requirements put in place by SOX are that record keeping and data integrity are critical.

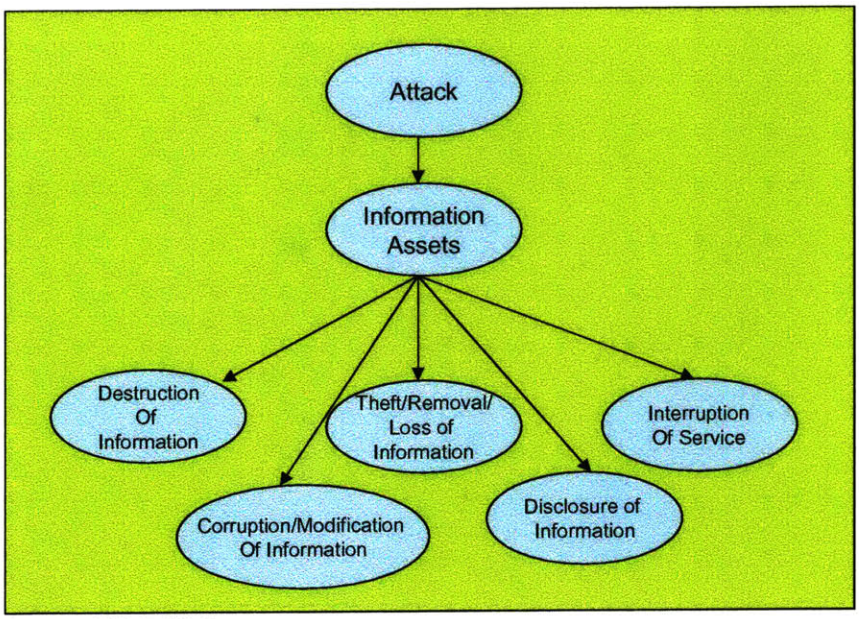
Regulations around data protection are also important to be considered in the context of supply chain. Systems which contain individual customer data are also being subject to regulations. Recent laws passed in California (California Security Breach Information Act, Senate Bill 1386 of 2002) and being proposed nationally have made it necessary for companies to divulge any security breach resulting in the disclosure of personal information. Companies that supply hospitals with patient specific goods, such as medical surgical supplies, may also have to comply with the standards for protecting data as defined in HIPAA.

3 Literature Review

3.1 Classification of Information Security Incidents

In order to discuss information security risk, we must first establish a classification of threats. One method for the classification of threats is set out in the ISO7498-2 document. It defines risk to information assets as the destruction of information, corruption/modification of information, the theft, removal or loss of information, the disclosure of information and the interruption of services as shown in Figure 1.

Figure 1: ISO 7498-2 Classification of Information Security Threats



Source: ISO 7498-2

Farahmand and Navathe (2002) present a more detailed method of classifying threats. They look at security threats with regard to two factors, the threat agent and the penetration technique. In

their view a threat is executed by a threat agent employing a technique. Threat agents are described as one of three types, unauthorized user, authorized user and environmental factors.

Table 1: Threat Agent Description

THREAT AGENT	DESCRIPTON OF THREAT AGENT
Authorized Users	Authorized users be unwitting threat agents if they commit errors. Authorized users can also intentionally cause a threat if they exceed their privileges or authorization level.
Unauthorized Users	Unauthorized users are defined as anyone who interrupts the productivity of the system by either covert or over means.
Environmental Factors	Environmental influences such as fires or natural disasters such as floods.

Source: Farahmond and Navathe (2003)

The techniques that are employed by threat agents to create the threat are described by Farahmond (2003) as physical, personnel, hardware, software and procedural. Physical techniques are as one would assume, gaining entry into a restricted area that to access a computer room or other sensitive area. The threat from personnel can be manifested in two ways, a malicious threat and an unwitting threat. The malicious threat is that of an employee that is either disgruntled or can obtain some benefit from an attack, either assists an outsider or executes an attack. Employees can also be tricked into performing a malicious act without their knowledge. This is often referred to as social engineering. Social engineering can be performed in a phone call asking for details about the company or can be elaborate schemes that involve long time frames and the development of relationships with the staff. Hardware and software techniques simply refer to the attacks that can be mounted against these assets. The threat from procedures is the one of authorized or unauthorized users penetrating a system due to a lack of controls, such as password policies not being enforced.

The method that seems to the author to be the most comprehensive in defining a framework within which to describe information security risk is one defined by Howard and Longstaff

(1998). This method looks at security breaches from the perspective on security incidents which are made up of attacks and their corresponding events. This method gives a framework for best describing the context and outcomes of security events. The reason for this method being preferred beyond its comprehensive nature is that it provides an ability to put into context data that is generated by security devices that are widely deployed throughout company networks. This framework will be further discussed in Chapter 3.

3.2 Impact of Security Breaches

There has also been some work done assessing the financial impact of information security breaches, although none of it specific to supply chain applications. Garg, Curtis, and Halper (2003) state that most previous work quantifying the financial impact of information security breaches has been through the analysis of self-reporting surveys conducted by CERT, the FBI and other organizations. Garg et al (2003) sought to determine the financial impact of a security breach by using an event-study methodology. By observing the impact on a company's performance in the public markets following the publication of a non-virus related information security event, they hoped to determine the financial impact of such a breach. They found that security breaches did have an impact on financial performance ranging from a relatively minimal average effect of 1.1 percent reduction in share price over three days for web defacement attacks to 36 percent reduction in share value over three days for Egghead following an incident that put customer credit card information at risk. The type of company also had an impact on the severity of a market response to an event, whereas the average response to a web-defacement was a 1.1 percent drop in share price, while an Internet security company, RSA lost 17.1% of their market cap value following a web-defacement (Garg 2003).

Garg et al (2003) classified incidents in the following manner:

1. Web site defacement
2. Denial of service
3. Theft of customer information
4. Theft of credit card information

They found that the theft of credit card information had the most negative impact on stock performance, most likely because of the perceived liability for the company from such a threat. The type of companies examined in the Garg et al (2003) study is deemed to be Internet dependent firms including: Staples, Travelocity, Yahoo, Microsoft, Time Warner and Diageo. While this study does have an interesting method for quantifying reputation issues, it does not address issues that do not become public. It also does not address issues where there is a disruption of service.

Another approach to quantifying information security risk was performed by Gordon and Loeb (2002). They looked to derive an equation that could be used to evaluate the level of investment that a company should invest in information security. The three main parameters "the loss conditioned as a breach occurring, the probability of a threat occurring and the vulnerability, probability that that a threat would be successful". By not taking into account the monetary loss, this model does not serve as a good tool for quantifying the security risk to companies.

3.3 Risk Assessment

Risk is commonly defined as a measure of probability and severity of adverse effects (Lowrance 1976). Quantitative risk analysis usually relies on probability and statistics derived from "historical data, statistical analysis, and/or systemic observations and experimentation" Yacov (1998). Probabilities determined by these methods are referred to as objective probabilities. In

cases where there is little historical data and experimentation is impractical, one can rely on subjective probabilities. Information security incidents are outcomes that are best described by subjective probabilities. There is very little historical data and no way to experiment on a live system in a way to generate a probability.

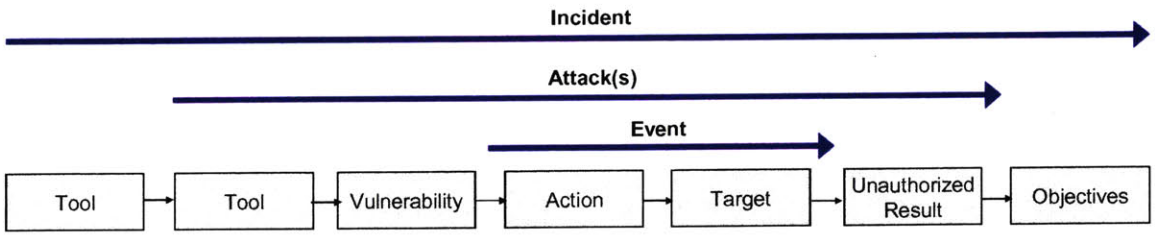
The ultimate purpose of any risk analysis and the resulting decision making process should be to answer the fundamental question posed by Lowrance: "Who should decide on acceptability of what risks, for whom, in what terms and why?" (1976) The impact of information security incidents can be a denial of service that makes it difficult for trading partners to interact or an information disclosure or integrity issue which may cause a loss in confidence of trading partners. Since these incidents may impact supply chain partners, the question of acceptability of risk of incurring these impacts should be discussed not only within the information security department, but also considered by those with responsibility for supply chain relationships that may be impacted by an incident.

4 Information Security Risk

4.1 Detailed Description of Information Security Classification

It is important to define a set of terms and a framework to discuss information security. One way of looking at information security is to think about events which security devices can record in the form of alerts and logs. A series of events and their surrounding context compose an attack. An attack or series of attacks that are initiated for a reason are an incident. When considering an incident, the analysis moves beyond the what, where and how of the attack to concentrating on who performed the attack and the motivation (why) for initiating the attack. This classification schema is illustrated in the diagram below:

Figure 2: Sandia Computer and Network Incident Taxonomy

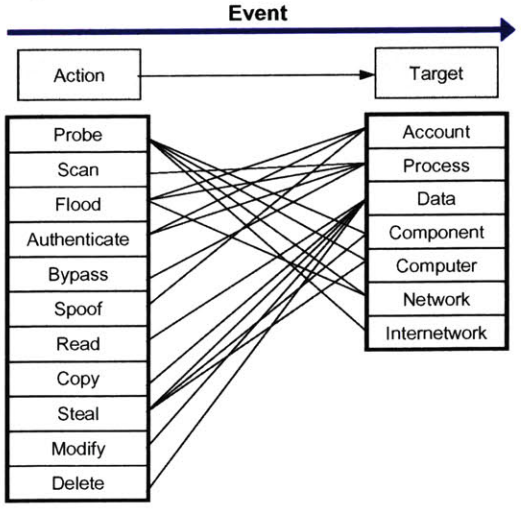


Source: Howard and Longstaff, 1998

4.2 Events

Considering an incident is made up of events, which are composed of an attack or multiple attacks, one can understand an incident by examining its most basic unit, the event. An event can be defined as an action taken to access a target, which results in a change of the state or status of the system or device being targeted. An example of an event would be the action of a scan being run against a network, the target. Another example would be the action of authentication being performed on an account, the target. When looking at events, we can classify all of them as being composed of one of the following actions: probe, scan, flood, authenticate, bypass, spoof, read, copy, steal, modify or delete. These actions can be authorized or unauthorized, which is defined by being approved or unapproved by the owner or administrator of the target. The targets for the actions can be one of the following: an account, process, data, component, computer, network or internetwork. Not all combinations of actions and targets are possible or even likely. The diagram below indicates the most common combinations.

Figure 3: Event Scenarios – Logical action and target combinations



Source: Modified from Howard and Longstaff, 1998

Most events that occur on computers and networks are routine and of no interest in the context of security analysis. An authorized user that authenticates their account is an event which would not be of interest. Thousands of these events occur every day; the identification of events that are unauthorized and outside of normal operations is the reason that security devices such as Intrusion Detection Sensors (IDS) and Firewalls are deployed on networks. An event becomes of interest to a security professional when it constitutes or is part of an attack. We will use IDS generated events as an indicator of the probability of an attack being carried out later in the paper.

4.3 Attacks

An attack is executed by the assembly of a series of steps by an attacker in order to realize an unauthorized result. In the framework proposed by Sandia (Howard and Longstaff, 1998), attacks are characterized by the logical steps that an attacker assembles. According to the framework, the attacker uses a tool to exploit a vulnerability. The tool creates an action against a target resulting in an unauthorized result. An attacker uses any of the following types of tools: physical attack, an information exchange, user command, script or program, autonomous agent, toolkit, a distributed tool or a data tap.

Vulnerabilities are "a weakness in a system that allows unauthorized action"(Howard and Longstaff, 1998). According to Sandia's taxonomy, vulnerabilities can be divided into three categories. Design vulnerabilities are those which are the result of errors in the design or specification of hardware or software, which makes a target susceptible to attack. No amount of care taken during the installation or implementation will prevent a design vulnerability. Vulnerabilities that result from improper implementation of hardware or software are described as implementation vulnerabilities. An error in the configuration, such as having a system account

with a default password, is defined as a configuration vulnerability (Howard and Longstaff, 1998).

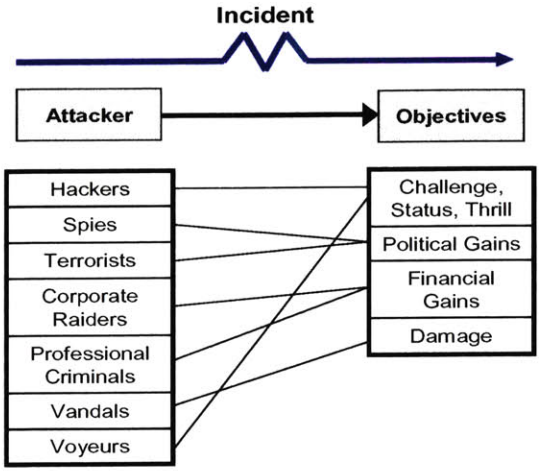
A successful attack is characterized by the attacker's steps, including the use of a tool to exploit a vulnerability in order to perform an action on a target, resulting in an unauthorized result. Unauthorized results include an increase in accessibility, a loss of confidentiality, a loss of information integrity, a denial of service and the theft of resources. An increased accessibility means that an attacker has increased his level of access to an unauthorized level on a computer or network. The loss of confidentiality and information integrity involves the distribution of information to any party not authorized and the corruption of data on a computer or network. A denial of service is characterized by the "intentional degradation or blocking of computer or network resources". A theft of resources is the unauthorized use of resources such as bandwidth on a network.

4.4 Incidents

An incident is the context around an attack that allows it to be grouped with other attacks based on the attacks being performed, their objectives, the sites or the timing are referred to as an incident. An incident can be characterized by the type of attacker and the objective. The type of attacker is an important part of determining the attacker's motivation and his subsequent objective. Within the Sandia taxonomy, types of attackers are identified as hackers, spies, terrorists, corporate raiders, professional criminals, vandals and voyeurs. Like there being some logical and illogical combinations of actions and events, similar relationships can be drawn between the type of attacker and their objective. For example, a professional criminal's primary objective will be financial gain, whereas a vandal will seek to achieve a challenge, status and

thrill and to create damage. The most common relationships between an attacker and the objective are shown in Figure 4.

Figure 4: Attacker and Objectives Relationship



Source: Modified from Howard and Longstaff, 1998

4.5 Examples of Adverse Effects of Unauthorized Results to a Supply Chain

4.5.1 Disclosure of Information

After virus infections and employee abuse of Internet access, unauthorized disclosure of information incidents were the third most common information security incidents experienced by firms responding to the 2004 CSI/FBI Computer Crime and Security Survey, with 59% of firms surveyed reporting these types of attacks (Gordon, Loeb, Lucyshyn, Richardson, 2004). The impact of the disclosure of information to members of a supply chain can be grouped into two categories, disclosure of a partner's information and disclosure of internally sensitive information. An obvious example of an information disclosure incident is the disclosure of

client's credit card numbers. The consequences of such a disclosure would be the loss of customer trust and an avoidance of doing business in the future.

In the context of a business to business relationship, an information disclosure incident that would have an impact on the supply chain would be the disclosure of client pricing information. The disclosure of this sensitive client information could lead clients to lose confidence in their supplier and potentially end a relationship. The pricing visibility could also result in increased pricing pressure on the supplier leading to lower margins for the business.

4.5.2 Corruption of Information

An information security breach that resulted in the corruption of information could be particularly damaging to a company's relationships with supply chain partners and result in additional costs due to correcting errors resulting from the incident. An information security breach that resulted in the corruption of order data could lead to orders being improperly fulfilled, delivered or billed. One can imagine the impact of a truckload of a critical raw material being shipped to another location. Not only would the cost of reshipping the material be an issue, but the potential consumer of the raw material could experience operational issues as a result not receiving the shipment. If an information security incident at the supplier resulted in the corruption of order information, the supplier would bear additional costs to correct it and possibly face liability under contracts with their customers.

4.5.3 Denial of Service

A denial of service that would have an impact on the supply chain operations of a firm would be the loss of a system critical to supply chain activities. The inability to access a warehouse

management application would lead to the inability of a distributor to store and ship items. The delay of shipments to customers could result in additional costs for the expedited shipments of product or the loss of customers due to missed delivery dates. With 17% of firms that participated in the CSI/FBI Computer Crime and Security Survey reporting successful denial of service attacks, protecting against such an attack on systems critical to the sourcing, production planning, handling, order management and shipment of products should be considered important especially by those companies that consider the supply chain a competitive advantage. (Gordon, et al., 2004)

5 Methodology

The premise of this analysis is that a system is composed of assets. By examining the risk of information security breaches to each asset within a system, the overall risk of the system can be determined. The likelihood of an undesired outcome occurring to an asset can be modeled by looking at the vulnerabilities related to that asset. The probability of an asset being compromised can be estimated based on the availability and ease of performing the exploit, the frequency of the relevant attacks being observed in a variety of systems, and the attractiveness of the target. This probability of compromise is then combined with the possible loss or cost resulting from a security breach to determine a risk value for the asset. Totaling the expected values of loss assessed to the assets that comprise a system will give a risk value for each system. Using expected value of loss and the company's security priorities, risk mitigation plans within the resource constraints of the organization can be formulated.

5.1 Asset Identification

The first step in assessing a system's information security risk is identifying the assets that make up that system. It is important to know the status of all assets and their location within the network in order to begin to understand its criticality within the system. The complex nature of networks, which typically increases with the size of the corporation, makes the task of tracking assets that are deployed within a network non-trivial. The nature of the network is also not static because assets are constantly being added and removed. The security status of an asset can also

change, if a new vulnerability is released or if its location within the network is changed. In order to track these changes, many companies use an asset management system that is updated by regular network scans which will capture the true composition of assets in the network and highlight any new vulnerabilities.

For the purposes of this study, three hypothetical systems have been proposed, 1.) a manufacturer's order management system, 2.) a distributor's order management system and 3.) a customer's system for accessing the Internet to place orders and communicating with partners over email. These systems are very simple and do not reflect the impact that other assets within a network could have on the order entry systems, but the basic process involved of considering each asset or class of asset and determining the hardware, operating system, software packages and any corresponding vulnerabilities are the same within a hypothetical network and an actual operating network. The added complexity of an actual system would not only increase the work required to perform the asset and vulnerability identification phase of the evaluation, but also add another layer of complexity due to a greater number of possible interactions between assets.

5.1.1 The Manufacturer's Order Management System

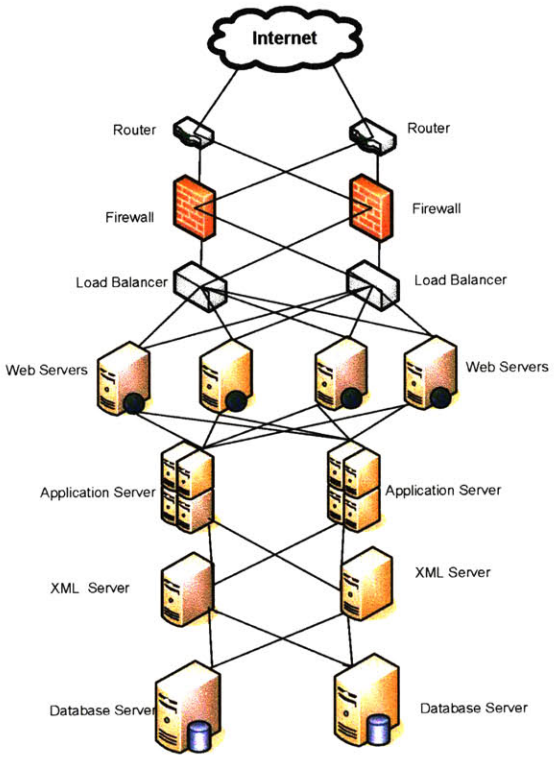


Figure 5: Network Diagram - Manufacturer's Order Management System

In order to evaluate the possible risk to the system, one must start with an understanding of the business processes that are supported and the data stored to support those processes. The hypothetical system proposed is an order management system built with redundant devices. The system is used by the manufacturer to transact annual revenues of $500 million. There are two Oracle databases which stores the customer and order information from their five hundred customers. Orders can be placed either through the web front end or via XML messaging which has been introduced with 70% of customers. The main application functionality is password protected.

5.1.2 The Distributor's Order Management System

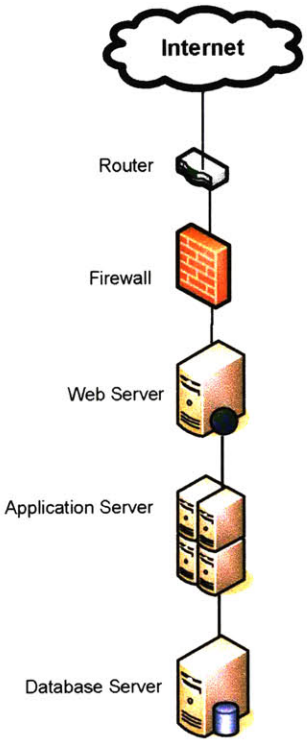


Figure 6: Network Diagram – Distributor System

The hypothetical distributor's network does not have redundant systems making it immediately simpler than the manufacturer's system. The system handles the $25 million dollars in revenue that is annually transacted by the distributor. The distributor has three thousand customers that are served primarily through the web front end of the order management system. The customer data and corresponding order information is stored in a SQL database.

5.1.3 The Customer's System for Trading Partner Communication

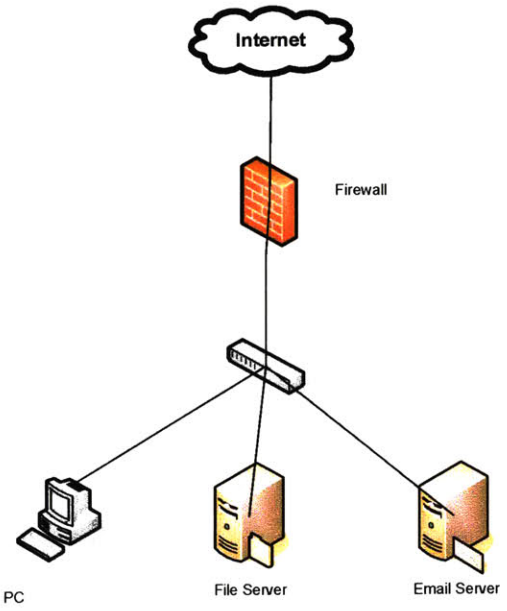


Figure 7: Network Diagram – Customer System

The hypothetical customer system is the least complex of the three systems. It includes a personal computer, a file server, router and a firewall. The customer uses the personal computers in their network to communicate with their supplier. They do not have any sort of web presence for communicating with customers. They do correspond with their 2500 customers via email to receive orders and confirm shipments.

5.2 Vulnerability Assessment

The next step in the assessment is to identify the vulnerabilities within the system through a combination of automated vulnerability scanning and manual penetration/vulnerability testing. As discussed in Chapter 4, vulnerabilities are "a weakness in the system allowing unauthorized action" (Howard and Longstaff, 1998). An automated vulnerability scan is a program that

systematically scans remote networks to identify vulnerabilities. There are a number of open-source and commercially available scanners including Nessus, nmap, ISS, CyberCop, Qualys and Bindview.

External scanning programs are only able to identify vulnerabilities that are detectable from the Internet. While this may seem sufficient, if there were to be an issue within the network such as the failure of a firewall or an attack was launched internally, the vulnerabilities that were not detected from an external scan would be accessible to an attacker, and thus need to be considered as a possible risk. Internal scanning should be performed in order to compile a complete inventory of the vulnerabilities within the system. In order to confirm vulnerabilities found via the scans, a manual security assessment is often performed to eliminate false positives, better identify possible attack vectors and carry out a detailed analysis of the vulnerabilities. Internal scanning can also be used as a tool for asset identification. When assessing a system that supports an e-commerce application such as those being described in the hypothetical manufacturer and distributor systems, an application assessment should also be performed to detect vulnerabilities, such as SQL injection, that may be present in a web-based application.

For the purpose of this study, vulnerabilities were assigned to appropriate assets within the hypothetical systems. The vulnerabilities that were attributed to the assets are commonly found network and application vulnerabilities. In order to focus the scope of the analysis, the vulnerabilities selected were those that would result in one of three outcomes: denial of service, loss of information integrity or information disclosure. In order to illustrate the impact of a compromise of to all of the critical assets, vulnerabilities were attributed to each type of asset in the hypothetical systems.

5.2.1 Probability of an Unauthorized Result

One of the challenges in modeling the risk of an information security breach is that deriving objective probabilities is difficult due to the lack of historical data and the impracticality of generating experimental data. In order to determine a probability to use for the quantitative risk assessment methodology described in this paper, each unauthorized result stemming from a vulnerability was given a score based on four characteristics. The total score was then used to determine the probability based on a linear relationship. The four characteristics that were scored were the ease of the exploit, the availability of the exploit, attractiveness of the target and the frequency of the attack Internet wide.

5.2.1.1 Ease of Exploit

An ease of exploit rating was assigned to each vulnerability based on the skill level an attacker must possess in order to perform the exploit. By rating the level of modification that would be required to use a tool or commonly known exploit method, one can get a measure of the skill level required to be successful in performing the attack. Further, the level of skill required gives an indication of the size of the pool of possible attackers. If there is no exploit available, the skill level required would be very high. This would make the size of the pool of potential attackers small and thus the likelihood that the attack would be successful low. An existing tool that does not require any modification would require a relatively low skill level. The lower skill level implies that there is a larger pool of individuals that could perform the attack and achieve the unauthorized result, and therefore the probability of a successful attack is high.

Table 2: Ease of Use Scoring Model

Score	Description of Ease of Exploit
5	No Modification Needed
4	Some Modification Needed, Information Available
3	Some Modification Needed, Information Unpublished
2	Exploit Exists but Unpublished
1	Exploit Not Available

5.2.1.2 Availability of Exploit

The availability of the exploit rating is applied in order to give an indication as to whether the exploit is widely available or not. Again, the more widely an exploit has been published the more likely the vulnerability will be attacked.

Table 3: Availability of Exploit Scoring

Score	Description of Availability of Exploit
5	Google Searchable
3	Published on Semi-Private Lists
1	Available only on Private Lists
0	No Known Exploit

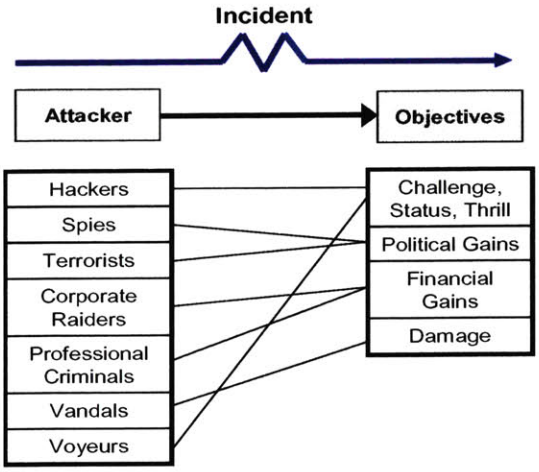
5.2.1.3 Attractiveness of the Target

When considering the attractiveness of the target, the perceived value of target was considered with respect to unauthorized result that an attack would achieve. Any evaluation of the perceived value must be somewhat subjective. By not basing the score solely on the target and including the possible outcome achieved by an attacker, there was an ability to be more specific in the scoring. For example, one might consider a router to be a less attractive target than a web server, because of its perceived criticality within a system. If the vulnerability that has been associated with the router allows an attacker to reroute incoming web traffic to a web site not managed by

the company that owns the system, it might be considered to be a very attractive target. The unauthorized result of such an attack could result in not only a denial of service to the company's system, but the possibility of customers being routed to a web site that could provide the attacker with a large financial gain or increase in status.

In order to understand the attractiveness of a target, the analysis must extend beyond the attack to the incident. When considering an incident, the context of an attack is considered including the type of attacker and the attacker's objective. As discussed in Chapter 4, Sandia has seven classes of attackers: hackers, spies, terrorists, corporate raiders, professional criminals, vandals and voyeurs (Howard and Longstaff, 1998). The relationships between attackers and their objectives are shown here again, as in Figure 4 in Section 4.4.

Figure 8: Attacker and Objectives Relationship



Source: Modified from Howard and Longstaff, 1998

In order to assess the attractiveness of a target, the first step is to determine the set of attackers that would be interested in the system in question. In the case of all of the hypothetical networks in this study, the attackers considered are hackers, professional criminals, vandals and voyeurs.

Spies and terrorists were eliminated from the analysis due to the lack of a political gain from a compromise of one of the systems being studied. There may be instances where a corporation would be the target for these types of attackers, but in this case the product being traded would not be of interest to such a group. A vulnerability and its corresponding unauthorized result is looked at from the perspective of each type of attacker and the level to which it satisfies his/her objective.

The two main attacker objectives that are relevant to most e-commerce enabled systems are "challenge, status and thrill" and "financial gain". When considering "financial gain", not only is the direct financial gain such as the transferring of funds relevant, but also the potential for financial gain through obtaining sensitive information, such as credit card numbers, which could be illegally used or sold. While the actual value of a financial gain can be roughly calculated, the "challenge, status and thrill" objective is very subjective. Two factors that can be considered to rate the attractiveness in terms of the "challenge, status and thrill" objective are the visibility of the unauthorized result and the profile of the company being attacked. The defacement of a web site is a very visible, thus it is fairly attractive to attack. If the web-site is the home page of a Fortune 500 company, it would be rated highly attractive. If it were the website of a small local paper distributor, it would be rated as medium or low attractiveness. The scale and corresponding attractiveness ratings are in Table 4 below.

Table 4: Attractiveness of Target Scoring

Score	Attractiveness of Target
5	High Impact
3	Medium Impact
1	Low Impact
0	No Impact

5.2.1.4 Frequency of Attack

The final rating applied to a vulnerability was the frequency of this attack occurring Internet wide. The method used for determining this relative frequency was through analyzing Intrusion Detection System (IDS) event logs collected from a set of 364 devices that provide representative sample of IDS devices being monitored by an independent security services firm. The IDS devices are part of the security infrastructure of a variety of Fortune 500 companies including automotive, financial services, media and retail companies. These devices were located both at the perimeter and in internal segments of the corporation's networks. The assumption being made is that these 364 sensors that are placed in a variety of environments throughout the world represent a good sample of the types of attacks occurring Internet wide.

Events from the 364 IDS sensors were gathered over a 31 day period from 24 February 2005 until 26 March 2005. The time frame of 31 days was selected in an attempt to go through a full monthly cycle of network activity, while keeping the amount of data manageable. During the 31 day period there were 115,655,000 events collected by all of the sensors. These events represented 3354 different attacks as detected by IDS signatures. The top 135 attacks represented 95% of the over all event volume.

In order to score the vulnerabilities that are being considered, a search of the event database is performed to determine if an event indicating an attack directed at that vulnerability is present. If an event that indicates this attack has been performed is found in the database, it is scored based on whether it is seen in the top 95% of events or not. If it is in the top 95%, it is rated as a "2". If it is not in the top 95%, it is rated as a "1". If it is not found, then it is rated as "0". If an analysis were being performed on a real system that has an IDS installation, a high score of "5" would be assigned if the attack was detected within the network.

Table 5: Frequency of Attack Internet Wide

Score	Frequency Measure
5	Event Seen in Target Network
3	Event seen and subject of Internet wide alert
2	Event in top 95% of Attacks
1	Event seen in bottom 5% of attacks
0	Event not seen

5.2.1.5 Probability Relationship to Outcome Score

In order to arrive at a probability of the vulnerability being exploited, the score from each of the four vulnerability characteristics, ease of use, availability, attractiveness of target and frequency, are totaled to determine the Vulnerability Base Score.

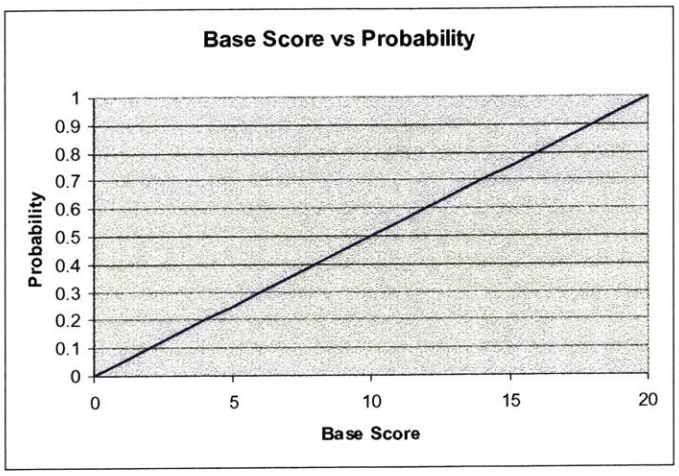
Equation 1: Vulnerability Base Score

$$E = \{1,2,3,4,5\}$$
$$A_v = \{0,1,3,5\}$$
$$A_t = \{0,1,3,5\}$$
$$F = \{0,1,2,3,4,5\}$$
$$V = E + A_v + A_t + F$$

Where V is Vulnerability Base Score, E is Ease of Use, A_v is Availability, A_t is Attractiveness, and F is Frequency.

The possible Vulnerability Base Scores were then assigned a probability based on a linear relationship, where the minimum possible score of 1 was assigned a probability of 0.05 and the maximum possible score of 20 was assigned a probability of 1.0.

Figure 9: Base Score and Corresponding Probability



5.2.2 Unauthorized Results Considered

In order to focus the scope of this model, the analysis was limited to evaluating the impact of three unauthorized results. If we refer back to the Sandia Model described in Chapter 4, there are five unauthorized results described in the security incident classification (Howard and Longstaff, 1998). By focusing on attacks that result in disclosure of information, corruption of information and denial of service, the analysis was narrowed to the results that would have the greatest impact on a supply chain, as the examples in Chapter 4 indicate. The two results not considered in this model were increased access and a theft of resources. The method for adding these two additional results to the model would not be difficult. The probability calculation would be the same and evaluating the impact of increased access of the additional results would simply be an extension of the logic used for the unauthorized results in this analysis.

5.3 Quantifying Impact on an Asset of an Unauthorized Result

In order to perform a quantitative risk assessment, there must be a probability of an outcome and a value of that outcome occurring. In this method, the value of the outcome occurring was determined by looking at each target and determining what the cost to the business would be for each of the unauthorized results being considered. In order to determine these losses or costs, the business process being supported, the impact on partnerships and any regulatory costs resulting from the unauthorized results were considered. By considering how the three possible unauthorized result scenarios, denial of service, loss of information integrity and loss of information confidentiality directed toward each asset would impact the business financially, the values of the consequences were determined. It may be that some scenarios cannot logically be applied to an asset. For example the compromise of a load balancer would not on its own be responsible for a loss of information integrity. In this case, the calculation of the cost of such an action would obviously not be addressed.

The costs or losses stemming from each unauthorized result to the hypothetical systems considered are explained using a database server from the manufacturer's system as an example. These costs should be used as a guideline. However, companies engaged in a risk assessment may identify additional costs and decide that some of those listed are not relevant. The process of determining the relevant costs is one that should be specified by each business undertaking a risk assessment.

When considering the value of the loss resulting from a denial of service, the criticality of the asset to the continued operation of the complete system is necessary in order to understand its impact on the business processes being performed on the system. Once that is determined, the

costs that would be incurred due to the loss of availability and the resulting system-wide impact can be assessed. In the case of a denial of service, we determine if the denial of service will result in a loss of the entire system availability or have a more isolated impact.

5.3.1 Costs Related to a Loss in Availability

When considering the database servers in the manufacturer's system, it was first determined that a loss of availability of both databases would result in the system not being able to function. The opportunity cost associated with unavailability impact would be the amount of revenue lost from the orders expected to transact during the outage that would not be transacted at a later point. The amount of revenue expected to be transacted is arrived at by calculating the average transactions over a time period multiplied by the length of time the system is predicted to be unavailable due to the outage. After calculating the value of the expected transactions, the percentage of those transactions that would not be recaptured once the system was again operational is estimated. This estimate of the probability is based on the strength of relationships with customers and the difficulty a customer would have switching suppliers. Since the manufacturer has a relatively small number of customers with a high average value of the order, one would assume that the majority of orders would be attempted again once the system was operational, so a small percentage is estimated.

5.3.2 Costs Related to a Loss of Information Integrity

When considering a loss of information integrity, the losses that were considered are the cost of customers lost due to a loss in confidence, regulatory penalty costs, and the estimated labor cost for restoring information integrity. By calculating the annual revenue derived from each customer and determining the portion of the total customers that would lose confidence in the

company due to a loss of information integrity, the value of lost customers can be found. Generally a larger company with an established reputation would be expected to lose a smaller percentage of customers. However, if there is a potential for the disclosure of highly sensitive material, the percentage might be large even if the company has an established reputation due to the customer base having a higher sensitivity to this type of breach.

The regulatory penalty that could be levied if information which was altered impacts the company's ability to accurately record financial results, should be provided by the accounting department within an organization. For the purposes of this study, a regulatory penalty of $1 million dollars was used when considering a loss of information integrity incident involving the hypothetical manufacturer's database.

The labor costs of repairing the system is a fairly straightforward calculation. In the case of repairing a database, one would determine the average hourly rate for a database administrator and then multiply it by the number of hours estimated to be necessary to repair a major information integrity incident. The estimate for the amount of time can be based on the number of records in a database.

5.3.3 Costs Related to a Loss of Information Confidentiality

The outcome from a loss of information confidentiality was determined to be customer defection. The cost of the defection of a customer was arrived at in the same way as the calculation for cost of a customer resulting from an information integrity issue. An assumption was made in the case of the hypothetical manufacturer that the number of customers lost based on an information disclosure would be less than the number of customers lost due to an information integrity issue.

In Appendix A, a sample calculation of the losses and costs resulting from the unauthorized results described above are displayed for the database in the hypothetical manufacturer's system.

5.3.4 Alternative Method for Calculating Consequences

As discussed in the literature review, Garg et al (2003) studied the impact that an information security breach had on a company's stock market price. If we assume that a drop in stock price is actually representative of the value lost to the company, the Garg et al article (2003) might provide values for the expected consequence in the absence of analysis of the individual company situation. By finding the stock price impact for a similar type of company in the study, a company could use the percentage drop in stock price and corresponding loss of value to the company as the consequence value.

5.4 Expected Value of Loss Calculation

The methodology to this point has been aimed at identifying all the assets in a system, identifying any vulnerabilities associated with those assets, attributing a probability of exploit to each vulnerability and calculating the monetary impact of an unauthorized result. In order to quantify the risk of a security breach, the variables that were derived through the methodology explained above are used to quantify the risk to the asset, the system and the supply chain.

Equation 2: Expected Value of Loss Calculation

$$E[A_i] = \sum_{j=1}^{k} P(V_{ij}) C_{ij}$$

$$E[S_i] = \sum_{i=1}^{n} A_i$$

$$E[SC_i] = \sum_{i=1}^{N} S_i$$

Where A_i is an Asset, $P(V_{ij})$ is the Probability of a Vulnerability, C_{ij} is the Consequence of the Vulnerability, S_i = is a System, and SC_i is a Supply Chain

In order to provide to provide a unit-less classification of the expected value of loss, each vulnerability was classified as "A", "B", "C" or "D" based on the percentage of annual revenue that the vulnerability's expected value of loss represented. The table below specifies the ranges for each classification.

Table 6: Classification of Expected Value of Loss as a Percentage of Annual Revenue

Classification	Expected Loss as Percentage of Annual Revenue
A	Greater than 10%
B	Greater than 5%
C	Greater than 0.05%
D	Less than 0.05%

5.5 Risk Mitigation Plan

A risk mitigation plan is developed by considering the risk value for an asset, the cost of reducing the risk and the priorities of the company. In order to understand how a company's priorities could shift the prioritization of security projects, four risk mitigation plans based on different corporate goals were assembled for each hypothetical system. The first goal considered was to minimize expected value of loss. The other plans considered focused on the scenario of a company having no tolerance for one unauthorized result. All of these plans were subject to a budgetary and human resource constraint.

The cost to mitigate each vulnerability was determined by assessing the number of hours required to fix the system, the cost of the labor required for the work and any capital expenditure that needed to be made. For example, a software upgrade may be required in order to mitigate a vulnerability. In order to perform an upgrade, the system will need to be backed up and then the upgrade performed. The amount of time to perform and upgrade was estimated to be 16 hours, not necessarily performed consecutively. Based on an estimate of the loaded cost of for an employee to perform this task, an hourly rate of $100 was used to perform the calculation. Therefore an upgrade would cost $1600.

In this study, the information security budgets for each hypothetical organization based on spending benchmarks. According to the 2004 CSI/FBI Computer Crime and Security Survey, the average percentage of a firm's information technology budget that is spent on information security is between 1-2% (Gordon, Martin, Lucyshyn and Richardson, 2004). According to Weil and Broadbent (1998), manufacturing organizations, like the hypothetical manufacturer in this study, allocate an average 3.4% of their annual revenues to information technology budgets. Organizations in the wholesale and retail sector spend less on information technology. "Wholesalers" and "retailers" spend an average of 2.5% of annual revenues on information technology (Broadbent and Weil, 1998). If this study were being performed for an actual organization, this figure would simply be the budget allocated by the organization for information security.

6 Sample Risk Assessment

In this section, the results from the phases of the risk assessment on the three hypothetical systems, manufacturer's order entry system, distributor's order entry system, and customer network will be discussed and displayed as it would be in a report detailing the risk assessment.

6.1 Asset Identification

Lists of each asset that is deployed within the three systems were compiled based on the sample network diagrams.

Table 7: Asset Inventory List for the Three Systems

System	System Code	Class	Asset	Asset Code	Relevant Software
Distributor	DIS	Database	DB1	DISDB1	Microsoft SQL Server 2000
Distributor	DIS	WebServer	WS1	DISWS1	Apache 2.0.35
Distributor	DIS	Application Server	APS1	DISAPS1	Sun Microsystems Java System Application Server 7 Platform Edition Update 4
Distributor	DIS	Firewall	FW1	DISFW1	CheckPoint Firewall -1
Distributor	DIS	Firewall	FW1	DISFW1	CheckPoint Firewall -1
Distributor	DIS	Router	RT1	DISRT1	D-Link Router
Manufacturer	MFR	Database	DB1	MFRDB1	Oracle
Manufacturer	MFR	Database	DB2	MFRDB2	Oracle
Manufacturer	MFR	WebServer	WS1	MFRWS1	Appache 2.0.45
Manufacturer	MFR	WebServer	WS2	MFRWS2	Appache 2.0.45
Manufacturer	MFR	WebServer	WS3	MFRWS3	Appache 2.0.45
Manufacturer	MFR	WebServer	WS4	MFRWS4	Appache 2.0.45
Manufacturer	MFR	Router	RT1	MFRRT1	Cisco 7206VXR Router
Manufacturer	MFR	Router	RT2	MFRRT2	Cisco 7206VXR Router
Manufacturer	MFR	Application Server	APS1	MFRAPS1	Sun Microsystems Java System Application Server 7 Platform Edition Update 4
Manufacturer	MFR	Application Server	APS2	MFRAPS2	Sun Microsystems Java System Application Server 7 Platform Edition Update 4
Manufacturer	MFR	Load Balancer	LB1	MFRLB1	Zeus Load Balancer
Manufacturer	MFR	Load Balancer	LB2	MFRLB2	Zeus Load Balancer
Manufacturer	MFR	Firewall	FW1	MFRFW1	Cisco PIX 535
Manufacturer	MFR	Firewall	FW2	MFRFW2	Cisco PIX 535
Customer	CUS	File Server	FS1	CUSFS1	Windows NT
Customer	CUS	Email Server	ES1	CUSES1	Windows 2003/Exchange Server
Customer	CUS	Firewall	FW1	CUSFW1	Cisco Pix 501
Customer	CUS	PC	PC1	CUSPC1	Windows 2003/MSFT Office/Yahoo Instant Messenger

6.2 Vulnerability Assessment

The vulnerabilities that were used to evaluate the three systems were based on common vulnerabilities found in the Open Source Vulnerabilities Database (OSVDB, 2005), Sans Top 20 List (SANS, 2005), and Hacking Exposed for Applications (Scambray and Shema, 2002). The assets with an associated vulnerability are listed with a title, description, the generic unauthorized result description, brief mitigation description and a reference. There were eight vulnerabilities identified that affected twenty-one of the assets within the systems. A table including the reference URL for each vulnerability can be found in Appendix B.

Table 8: Manufacturer System Vulnerabilities Identified

Asset Code	Relevant Software	Vulnerability Name	Vulnerabilty Description	Reference Number
MFRDB1	Oracle	SQL Injection	SQL Injection poosible in all application input fields	Hacking Exposed
MFRDB2	Oracle	SQL Injection	SQL Injection poosible in all application input fields	Hacking Exposed
MFRWS1	Appache 2.0.45	Apache 2 apr-util IPV6 Parsing DoS	IPv6 URI parsing routines in the apr-util library for Apache HTTP Server and IBM HTTP Server contains a flaw that may allow a remote denial of service	OSVDB/ID: 9994
MFRWS2	Appache 2.0.45	Apache 2 apr-util IPV6 Parsing DoS	IPv6 URI parsing routines in the apr-util library for Apache HTTP Server and IBM HTTP Server contains a flaw that may allow a remote denial of service	OSVDB/ID: 9994
MFRWS3	Appache 2.0.45	Apache 2 apr-util IPV6 Parsing DoS	IPv6 URI parsing routines in the apr-util library for Apache HTTP Server and IBM HTTP Server contains a flaw that may allow a remote denial of service	OSVDB/ID: 9994
MFRWS4	Appache 2.0.45	Apache 2 apr-util IPV6 Parsing DoS	IPv6 URI parsing routines in the apr-util library for Apache HTTP Server and IBM HTTP Server contains a flaw that may allow a remote denial of service	OSVDB/ID: 9994
MFRRT1	Cisco 7206VXR Router	Apache 2 apr-util IPV6 Parsing DoS	TCP stack implementation of numerous vendors contains a flaw that may allow a remote denial of service	OSVDB/ID: 4030
MFRRT2	Cisco 7206VXR Router	Apache 2 apr-util IPV6 Parsing DoS	TCP stack implementation of numerous vendors contains a flaw that may allow a remote denial of service	OSVDB/ID: 4030
MFRAPS1	Sun Microsystems Java System Application Server 7 Platform Edition Update 4	Sun Java System Web / Application Server Malformed Client Certificate DoS	The issue is triggered by the use of malformed client certificates, and will result in loss of availability for the server.	OSVDB/ID: 11383
MFRAPS2	Sun Microsystems Java System Application Server 7 Platform Edition Update 4	Sun Java System Web / Application Server Malformed Client Certificate DoS	The issue is triggered by the use of malformed client certificates, and will result in loss of availability for the server.	OSVDB/ID: 11383
MFRFW1	Cisco PIX 535	ICMP Implementation Malformed Path MTU DoS	Triggered due to the handling of ICMP error messages and when the "Path MTU Discovery" (PMTUD) mechanism is used	OSVDB/ID: 15619
MFRFW2	Cisco PIX 535	ICMP Implementation Malformed Path MTU DoS	Triggered due to the handling of ICMP error messages and when the "Path MTU Discovery" (PMTUD) mechanism is used	OSVDB/ID: 15619

Table 9: Distributor System Vulnerabilities Identified

Asset Code	Relevant Software	Vulnerability Name	Vulnerability Description	Reference Number
DISDB1	Microsoft SQL Server 2000	Cross Site Scripting	Malicious code inserted due to lack of validation parameters leading making it possible for user's to see each other's accounts.	Hacking Exposed
DISWS1	Apache 2.0.35	Apache 2 apr-util IPV6 Parsing DoS	IPv6 URI parsing routines in the apr-util library for Apache HTTP Server and IBM HTTP Server contains a flaw that may allow a remote denial of service	OSVDB/ID: 9994
DISAPS1	Sun Microsystems Java System Application Server 7 Platform Edition Update 4	Sun Java System Web / Application Server Malformed Client Certificate DoS	The issue is triggered by the use of malformed client certificates, and will result in loss of availability for the server.	OSVDB/ID: 11383
DISFW1	CheckPoint Firewall -1	HTTP Server Format String	Check Point FireWall-1 HTTP Server Format String	OSVDB/ID: 4414
DISFW1	CheckPoint Firewall -1	HTTP Server Format String	Check Point FireWall-1 HTTP Server Format String	OSVDB/ID: 4414
DISRT1	D-Link Router	D-Link Router DHCP Request Flood DoS	D-Link Router DHCP Request Flood DoS	OSVDB/ID: 7287

Table 10: Customer System Vulnerabilities Identified

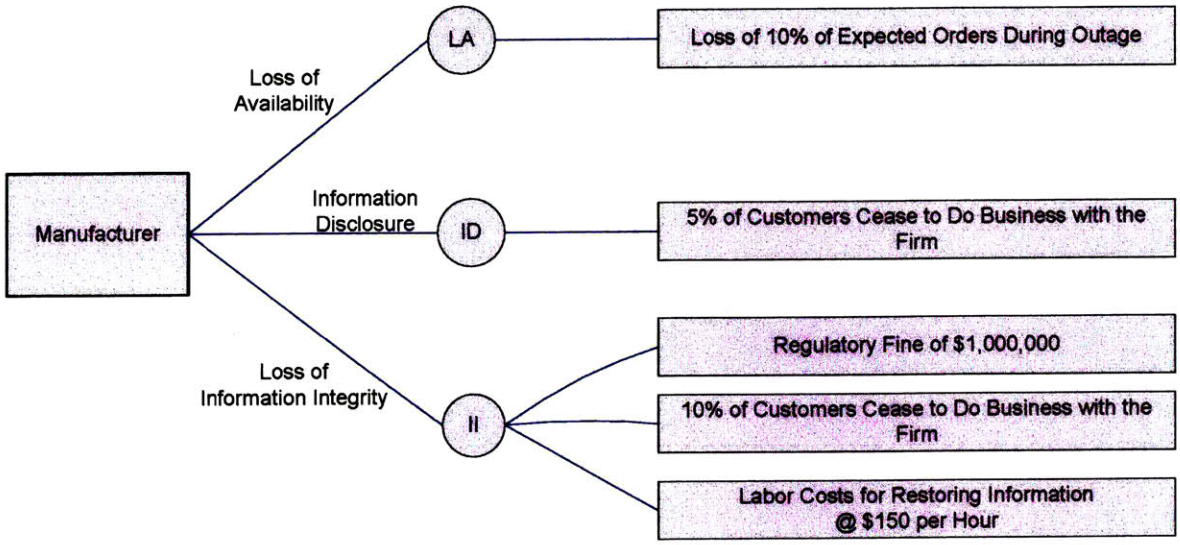
Asset Code	Relevant Software	Vulnerability Name	Vulnerabilty Description	Reference Number
CUSES1	Windows 2003/Exchange Server	ICMP Implementation Malformed Path MTU DoS	Triggered due to the handling of ICMP error messages and when the "Path MTU Discovery" (PMTUD) mechanism is used	OSVDB/ID: 15619
CUSFW1	Cisco Pix 501	ICMP Implementation Malformed Path MTU DoS	Triggered due to the handling of ICMP error messages and when the "Path MTU Discovery" (PMTUD) mechanism is used	OSVDB/ID: 15619
CUSPC1	Windows 2003/MSFT Office/Yahoo Instant Messenger	Buffer Overflow	Old version of Yahoo Messenger	SANS 20 and Bugtraq/ID 9145

6.3 Quantifying the Impact on Asset of Unauthorized Result

In order to examine the possible impacts of the unauthorized results on each asset, a result tree for each asset was developed. The results trees were developed based on estimates of the reaction of customers to the event, corporate responses to events, and regulatory fines levied. The possible reactions of customers that were considered were a decision to choose another supplier in the short term and the decision to discontinue the relationship entirely.

6.3.1 Manufacturer System Outcomes

Figure 10: Manufacturer's System Outcomes from Undesired Results



In the case of the manufacturer's system, it was determined that a loss of availability which made the order entry system inaccessible would result in 10% of the orders that should have placed during that time frame not being placed. The scenario that is assumed is that 10% of distributors that have difficulty placing their order through the system due to the outage, will choose to move that order to another supplier. In the case of the manufacturer, where they have relatively few customers, a relatively strong partner relationship is expected, and thus there is not expectation that the loss of availability will not lead to a long term customer loss. The cost of losing 10% of the orders for the affected time period was simply calculated based on the value of 10% of the order revenue that would be placed during a one day time period.

For the purpose of this analysis, a one day loss of availability was used. If it was perceived that due to the skills internal to the organization or severity of a possible attack the organization

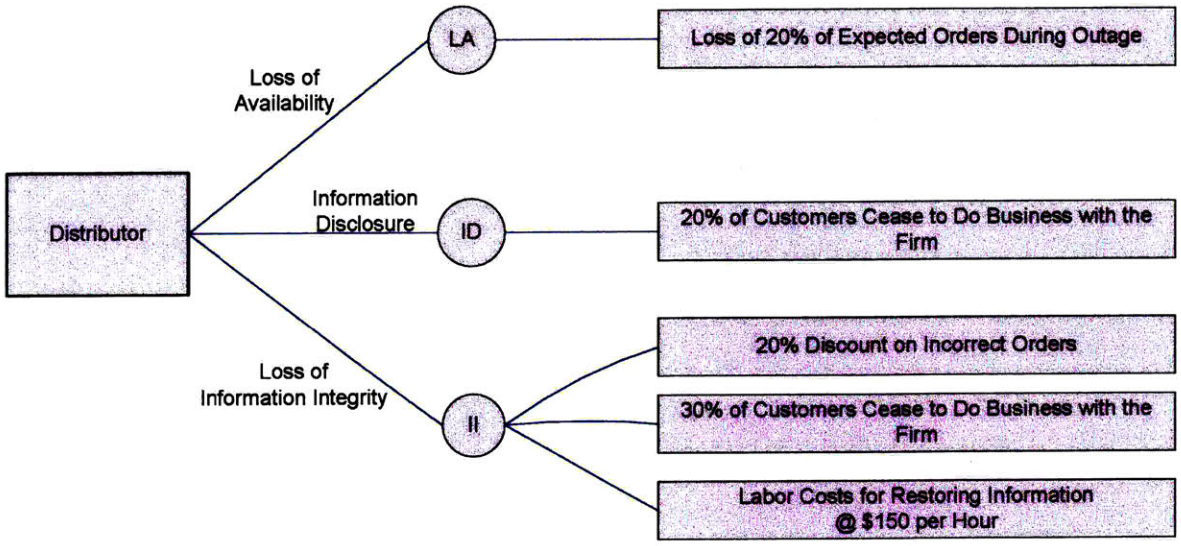
would take longer to recover, the time period could be extended and the calculation could be easily adjusted.

In the event of the manufacturer disclosing confidential data, it is perceived that 5% of the manufacturer's customers will lose confidence in the manufacturer and terminate their relationship. For this assessment, it has been determined that the loss of information integrity would result in more than just a loss of manufacturer customers. In the case of the manufacturer, an information integrity issue would result not only in a higher percentage, 10%, of customers terminating their relationship with the business, but there would also be regulatory and labor costs to consider..

In the event of a loss of information integrity, there would need to be the involvement of a database administrator or other skilled resource to try and restore the effected data. The hourly wage of a database administrator was estimated at $150. In addition, if there is difficulty restoring data completely, it may be prevent the firm from being able to accurately report their financial standing. In the case of the manufacturer, the potential fine from a violation of the Sarbanes Oxley Act of 2002 due to a misreporting of results was estimated at $1,000,000 per incident (Gegten, 2005).

6.3.2 Distributor System Outcomes

Figure 11: Distributor's System Outcomes from Undesired Results



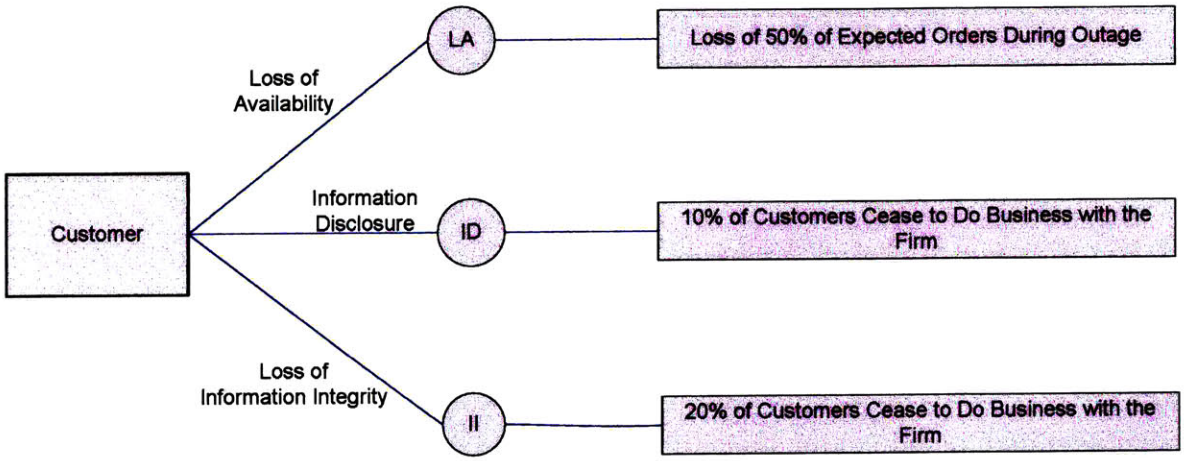
It can be noted that in the case of the distributor, the outcomes from each unauthorized results are more severe in terms of higher percentages of customers lost due information disclosure and integrity issues, and a higher percentage of orders that are switched to another supplier after a loss of availability. The logic applied is that the relationships with customers will not be as strong as there is a much larger customer base, and that the reputation of the company will be more easily damaged due to them being smaller and potentially perceived as less established.

In the event of a loss of availability of their systems, there is an expectation that 20% of the expected orders for that period of time will be switched to a competitor. In contrast to the manufacturer, the distributor in this case has a policy of giving a 20% discount on all orders incorrectly processed due to distributor error. In order to account for this in the model, the

outcomes from the loss of information integrity event are a loss of 30% of the customer base and a 20% discount to all orders that are affected. In this model, we used the assumption that only orders that were placed during the one day effected period were subject to this charge, but if other assumptions were made, such as the database corruption affecting more than just the orders placed during the incident, the loss from this policy could potentially be much higher. In the event of information disclosure, the assumption was that there would be a loss of 20% of the customer base.

6.3.3 Customer System Outcomes

Figure 12: Customer's System Outcomes from Undesired Results



The customer system was assessed to have a higher likelihood of customers switching to another source of their product were there to be a loss of availability. Instead of the 10% and 20% loss as seen in the manufacturer and distributor respectively, the customer would be expected to lose 50% of expected orders. In the case of a loss of information integrity the customer is expected to only lose 20% of their customer base, due to their average order size being small enough that their customer's perception of risk related to continuing to work with them would be relatively

small. In the case of information disclosure, the loss was estimated to be 10% of the customer base.

6.3.4 Risk Rating – Calculation of the Expected Loss

Once the outcomes for the three unauthorized results were determined, they were then mapped to the vulnerabilities that had been associated with each asset. Then the probability of the attack occurring were multiplied with the consequence to arrive at the expected value of the loss. A unit-less classification of the expected value of loss values was assigned in order to give reference to the severity of the expected loss in relation to the company's annual revenue. Each expected value of loss was assigned a letter, "A", "B", "C" or "D" based on the percentage of annual revenue. Table 11 defines the ranges for each classification. It is followed by Table 12 which displays the assets, with corresponding expected values of the loss and a classification of the value in terms of its percentage of annual revenue for each system.

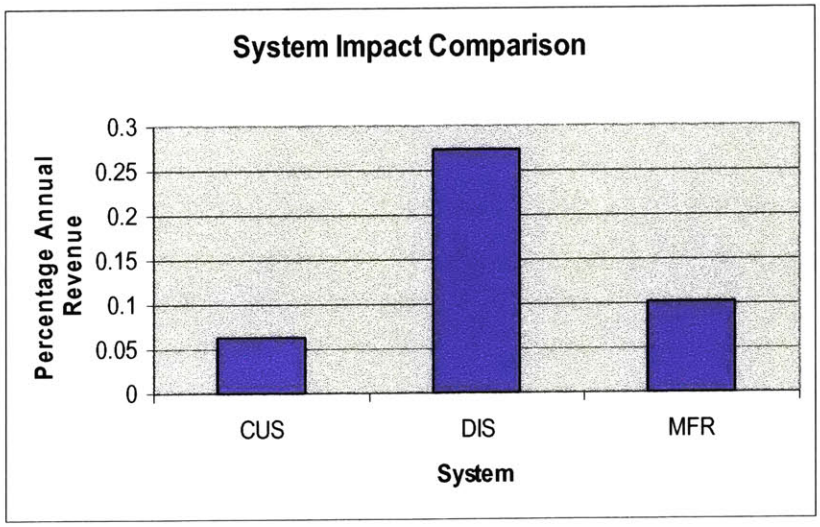
Table 11 : Classification of Expected Value of Loss as a Percentage of Annual Revenue

Classification	Expected Loss as Percentage of Annual Revenue
A	Greater than 10%
B	Greater than 5%
C	Greater than 0.05%
D	Less than 0.05%

Table 12: Vulnerabilities and Corresponding Expected Value of Loss

Asset	Vulneability	Outcome	Probability of Outcome	Expected Value of Loss	Classification
DB1	Cross Site Scripting	Information Disclosur	0.6	3000000	A
WS1	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	0.5	10000	D
APS1	Sun Java System Web / Application Server Malformed Client Certificate DoS	Loss of Availability	0.65	13000	D
FW1	HTTP Server Format String	Information Integrity	0.5	3820000	A
FW1	HTTP Server Format String	Loss of Availability	0.5	10000	D
RT1	D-Link Router DHCP Request Flood DoS	Loss of Availability	0.55	11000	D
DB1	SQL Injection	Information Integrity	0.5	25560000	B
DB2	SQL Injection	Information Integrity	0.5	25560000	B
WS1	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	0.5	25000	D
WS2	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	0.5	25000	D
WS3	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	0.5	25000	D
WS4	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	0.5	25000	D
RT1	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	0.65	65000	D
RT2	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	0.65	65000	D
APS1	Sun Java System Web / Application Server Malformed Client Certificate DoS	Loss of Availability	0.65	65000	D
APS2	Sun Java System Web / Application Server Malformed Client Certificate DoS	Loss of Availability	0.65	65000	D
FW1	ICMP Implementation Malformed Path MTU DoS	Loss of Availability	0.8	80000	D
FW2	ICMP Implementation Malformed Path MTU DoS	Loss of Availability	0.8	80000	D
ES1	ICMP Implementation Malformed Path MTU DoS	Loss of Availability	0.8	19000	C
FW1	ICMP Implementation Malformed Path MTU DoS	Loss of Availability	0.8	19000	C
PC1	Buffer Overflow	Information Integrity	0.25	150000	B

Table 13: Comparison of Percentage Annual Revenue at Risk Across the Three Systems



As can be seen in Table 13 above, in this model the distributor is at a much higher risk due to security breaches than the manufacturer or the customers. This is due in part because of the outcomes and consequences that were assessed to the system. As mentioned above, the rate of partner defection was higher at the distributor than at the manufacturer and the customer. The distributor was deemed to have less solid relationships with partners than the manufacturer, while at the same time the distributor's order value is such that the perceived risk to a partner after an incident would be high enough that the distributor would lose a greater percentage of its customer base than expected within the customer business. The assumption in this study was that redundancy does not reduce the overall expected loss security if the vulnerability exists on all assets performing the same function. It does however reduce the specific asset's expected loss, as the expected loss is divided between the two assets performing the same function. Redundancy is important in protecting systems from downtime due to mechanical failure, but if two assets have the same vulnerability and they are subject to an attack the assumption made in this study is that both would be attacked in the same manner.

6.4 Risk Mitigation Plans

6.4.1 Scenarios

Risk mitigation plans for each company were developed based on four different scenarios, minimizing expected loss value and then prioritizing each of the unauthorized results, loss of availability, loss of information integrity, and information disclosure. The plans were also compared to the information security budgets of each company as calculated based on benchmark percentages of annual revenues.

Table 14: Annual Security Budget Calculation

Company	Annual Revenue	% IT Budget*	IT Budget	% IT Budget for Security**	Security Budget
Manufacturer	$500,000,000	3.5%	$17,500,000	2.0%	$350,000
Distributor	$25,000,000	2.5%	$625,000	2.0%	$12,500
CUS	$3,000,000	2.5%	$75,000	2.0%	$1,500

*** Broadbent and Weil, 1998**
**** Gordon, et al., 2004**

The cost to mitigate the risk presented by each vulnerability was estimated based on the time to perform the action required, the cost of the labor and any capital investment required. The following table shows this calculation for all of the systems.

Table 15: Manufacturer Cost to Perform Mitigating Action

System	Class	Asset	Vulnerability Name	Outcome	Expected Value of Loss	Mitigating Action	Time to Repair	Hourly Wage	Labor Cost	Capital Cost	Total Cost
Manufacturer	Database	DB1	SQL Injection	Information Integrity	25560000	Programming	80	$150	$12,000	$0	$12,000
Manufacturer	Database	DB2	SQL Injection	Information Integrity	25560000	Programming	80	$150	$12,000	$0	$12,000
Manufacturer	WebServer	WS1	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	25000	Upggrade Software	16	$100	$1,600	$0	$1,600
Manufacturer	WebServer	WS2	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	25000	Upggrade Software	16	$100	$1,600	$0	$1,600
Manufacturer	WebServer	WS3	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	25000	Upggrade Software	16	$100	$1,600	$0	$1,600
Manufacturer	WebServer	WS4	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	25000	Upggrade Software	16	$100	$1,600	$0	$1,600
Manufacturer	Router	RT1	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	65000	Apply Available Patch	16	$100	$1,600	$0	$1,600
Manufacturer	Router	RT2	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	65000	Apply Available Patch	16	$100	$1,600	$0	$1,600
Manufacturer	Application Server	APS1	Sun Java System Web / Application Server Malformed Client Certificate DoS	Loss of Availability	65000	Upgrade Software	16	$100	$1,600	$0	$1,600
Manufacturer	Application Server	APS2	Sun Java System Web / Application Server Malformed Client Certificate DoS	Loss of Availability	65000	Upgrade Software	16	$100	$1,600	$0	$1,600
Manufacturer	Firewall	FW1	ICMP Implementation Malformed Path MTU DoS	Loss of Availability	80000	Upgrade Software	16	$100	$1,600	$0	$1,600
Manufacturer	Firewall	FW2	ICMP Implementation Malformed Path MTU DoS	Loss of Availability	80000	Upgrade Software	16	$100	$1,600	$0	$1,600

Table 16: Distributor Cost to Perform Mitigating Action

System	Class	Asset	Vulnerability Name	Outcome	Expected Value of Loss	Mitigating Action	Time to Repair	Hourly Wage	Labor Cost	Capital Cost	Total Cost
Distributor	Database	DB1	Cross Site Scripting	Information Disclosure	3000000	Programming	80	$150	$12,000	$0	$12,000
Distributor	WebServer	WS1	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	10000	Upggrade Software	16	$100	$1,600	$0	$1,600
Distributor	Application Server	APS1	Sun Java System Web / Application Server Malformed Client Certificate DoS	Loss of Availability	13000	Upgrade Software	16	$100	$1,600	$0	$1,600
Distributor	Firewall	FW1	HTTP Server Format String	Information Integrity	3820000	Apply Available Patch	24	$100	$2,400	$0	$2,400
Distributor	Firewall	FW1	HTTP Server Format String	Loss of Availability	10000	Apply Available Patch	24	$100	$2,400	$0	$2,400
Distributor	Router	RT1	D-Link Router DHCP Request Flood DoS	Loss of Availability	11000	Disable DHCP	4	$100	$400	$0	$400

Table 17: Customer Cost to Perform Mitigating Action

System	Class	Asset	Vulnerability Name	Outcome	Expected Value of Loss	Mitigating Action	Time to Repair	Hourly Wage	Labor Cost	Capital Cost	Total Cost
Customer	Email Server	ES1	ICMP Implementation Malformed Path MTU DoS	Loss of Availability	19000	Upgrade Software	16	$100	$1,600	$0	$1,600
Customer	Firewall	FW1	ICMP Implementation Malformed Path MTU DoS	Loss of Availability	19000	Upgrade Software	16	$100	$1,600	$0	$1,600
Customer	PC	PC1	Buffer Overflow	Information Integrity	150000	Upgrade Software	2	$100	$200	$0	$200

The following tables show the four mitigation plans for each system. The steps in the plan that fall outside of the budget, as shown above are shaded in red. Projects that will need to be scaled back to fall within budget are shaded pink.

6.4.2 Distributor Mitigation Plan

Table 18: Distributor Mitigation Plan with Budgetary Constraints

Asset	Vulnerability	Possible Outcome	Expected Value of Loss	%age of Overall Expected VOL	Class	Action	Total Cost	Minimize Expected Loss	Minimize Loss of Avail	Minimize Information Disclosure	Preserve Inforamation Integrity
FW1	HTTP Server Format String	Information Integrity	$3,820,000	56%	A	Apply Available Patch	2400	1	4	2	1
DB1	Cross Site Scripting	Information Disclosure	$3,000,000	44%	A	Programming	12000	2	5	1	2
APS1	Sun Java System Web / Application Server Malformed Client Certificate DoS	Loss of Availability	$13,000	0%	D	Upgrade Software	1600	3	1	3	3
WS1	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	$10,000	0%	D	Upggrade Software	1600	4	2	4	4
RT1	D-Link Router DHCP Request Flood DoS	Loss of Availability	$11,000	0%	D	Disable DHCP	400	5	3	5	5

The distributor's information security budget is $12,500. With the expected loss stemming from an event that causes either a loss of information integrity or information disclosure being so much higher than a loss of availability event, it would seem that the company should begin by

mitigating the firewall vulnerability. This vulnerability had a high expected loss because of the high consequence of an information disclosure and a probability of exploit of 65%. The relatively high probability was as a result of an exploit being available and a security device being an attractive target, resulting in high scores for the ease of use, availability, and attractiveness ratings. The Check Point Firewall-1 vulnerability allows a remote attacker to execute arbitrary code, which essentially means that the attacker can run any command they desire on the firewall (OSVDB, 2005). With administrative control of the firewall, the attacker could perform a denial of service or corrupt data passing through the firewall. The mitigation of the vulnerability can be performed by applying a patch provided by Check Point. The cost of applying the patch used in the model is calculated by estimating that a system administrator costing $100 would take 24 hours to test, implement, and document the patch release. The 56% reduction in the expected value of loss and relatively low mitigation cost of $2400 make it a logical first step in the mitigation plan.

The next project that the distributor should tackle, if the goal is minimizing expected value of loss, is the SQL injection vulnerability causing cross-site scripting. Cross-site scripting vulnerabilities are essentially an issue resulting from trusting foreign data. Through poor input validation in the database, an attacker can insert malicious code in the form of SQL commands to obtain other users data. The unauthorized outcome of information disclosure and the resulting attractiveness of the target resulted in the second highest expected value of loss in the system. Fixing this vulnerability is not as straightforward as applying a patch or upgrading an application. In order to address this issue, a programmer will need to ensure that there is validation of data in every place where the application accepts data. A programmer is a more expensive resource, costing an estimated $150 per hour, and it was estimated that there would be 80 hours of work

required to fix this problem. The resulting $12,000 mitigation cost will cause the distributor to be over budget. It may be possible to work with a programmer to determine how much could be accomplished and stay within the $10,100.

The remaining vulnerabilities in the system have the potential to cause a loss of availability and have significantly lower vulnerabilities that are classified in the "D" category. The Apache web server has a vulnerability which makes it possible for an attacker to formulate an attack using URI requests that causes a loss of availability of the server due to a crash of the httpd child process (OSVDB, 2005). This vulnerability can be fixed by upgrading the server to a later version. The Sun Java System application server in the system is also susceptible to a remote denial of service. This vulnerability is exploited through an attacker using malformed client certificates and can be mitigated through upgrading to the latest version of the software. The estimated of costs for upgrading each software package was based on an estimate 16 hours of work performed by an system administrator at a cost of $100 per hour.

The D-Link router in the system also has a vulnerability that may allow an attacker to perform a remote denial of service. By flooding the router with Dynamic Host Configuration Protocol (DHCP) packets, the attacker will cause the device to use all available memory, which will cause it to reboot (OSVDB, 2005). The repeated rebooting makes the router suffer a loss of availability. In the distributor network, where there is no DCHP server in use, this vulnerability can be mitigated by disabling DHCP. This is a straightforward task that should not take more than 4 hours of a system administrator's time, and thus costs $400 to fix.

6.4.3 Manufacturer

Table 19: Manufacturer Mitigation Plan with Budgetary Constraints

Asset	Vulnerability Name	Outcome	Expected Value of Loss	%age of Overall Expected VOL	Classification	Action	Total Cost	Minimize Expected Loss	Minimize Loss of Avail	Minimize Information Disclosure	Preserve Inforamation Integrity
DB1	SQL Injection	Information Integrity	$25,560,000	49%	B	Programming	$12,000	1	11	X	1
DB2	SQL Injection	Information Integrity	$25,560,000	49%	B	Programming	$12,000	2	12	X	2
FW1	ICMP Implementation Malformed Path MTU DoS	Loss of Availability	$80,000	0%	D	Upgrade Software	$1,600	3	1	X	3
FW2	ICMP Implementation Malformed Path MTU DoS	Loss of Availability	$80,000	0%	D	Upgrade Software	$1,600	4	2	X	4
RT1	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	$65,000	0%	D	Apply Available Patch	$1,600	5	3	X	5
RT2	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	$65,000	0%	D	Apply Available Patch	$1,600	6	4	X	6
APS1	Sun Java System Web / Application Server Malformed Client Certificate DoS	Loss of Availability	$65,000	0%	D	Upgrade Software	$1,600	7	5	X	7
APS2	Sun Java System Web / Application Server Malformed Client Certificate DoS	Loss of Availability	$65,000	0%	D	Upgrade Software	$1,600	8	6	X	8
WS1	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	$25,000	0%	D	Upggrade Software	$1,600	9	7	X	9
WS2	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	$25,000	0%	D	Upggrade Software	$1,600	10	8	X	10
WS3	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	$25,000	0%	D	Upggrade Software	$1,600	11	9	X	11
WS4	Apache 2 apr-util IPV6 Parsing DoS	Loss of Availability	$25,000	0%	D	Upggrade Software	$1,600	12	10	X	12

The manufacturer's budget of $350,000 is large enough to accommodate performing all of the actions required to mitigate the risk that has been identified in this system. The expected value of losses for the attacks involving information integrity issues are again, much higher than the loss of availability results. The vulnerability causing the potential information integrity issue is another SQL injection vulnerability causing the database to perform actions that are not part of the regular website operation. In this case, the SQL injection vulnerability can be exploited by an attacker that inserts nefarious commands into injection points, using generic error messages generated by the database in order to enumerate the tables in the database for further attack (Scambray and Shema, 2002). While the vulnerability is referred to as SQL injection, many databases including the Oracle database in the manufacturer's system are vulnerable to this phenomenon caused by insecure coding practices. The mitigation of this vulnerability requires a

programmer to make sure that any error messages returned by the database to the browser are generic, that the filtering of meta-characters is in place, that the type of input is defined in each parameter, and that the input meets that definition. For example, if a parameter is expected to be an integer and an input containing a non-integer is submitted, it should be discarded and a non-specific error returned. All parameters should also have maximum length defined. The cost of this project is the cost of a programmer at $150 per hour working for four weeks and totals $24,000.

The other vulnerabilities on the manufacturer's system all result in a loss of availability. The manufacturer's system shares two vulnerabilities with the distributor system. The manufacturer router and web servers are both are susceptible to the "Apache 2 apr-util IPV6 Parking DoS" (OSVDB, 2005) vulnerability. The manufacturer's application servers are also vulnerable to the Sun Java System server Malformed Client Certificate DoS. As described above, the mitigation of these vulnerabilities will cost $1600 per device.

The manufacturer's Cisco PIX 535 firewall is vulnerable to a denial of service attack caused by attackers sending ICMP messages that cause a reduction in the TCP connection throughput. The "ICMP Implementation Malformed Path MTU DoS" (OSVDB, 2005) affects multiple vendors including Cisco. This vulnerability has a high probability of being attacked due to the exploit being widely published and that the target, being a $500 million company's security device. This vulnerability requires an upgrade of the software, and therefore it has been assigned a cost of $1600 per device for testing, implementation and documentation of the upgrade process.

As there is no budgetary constraint on this mitigation plan, rather than using the plan to make choices, the manufacturer is in the enviable position of using it as a tool for the prioritization of

human resources. It would make sense for the manufacturer to employ a parallel effort to address the SQL injection vulnerability and the network infrastructure vulnerabilities at the same time, as the skill sets of the individuals working on each are different.

6.4.4 Customer

Table 20: Customer Mitigation Plan with Budgetary Constraints

Asset	Vulnerability Name	Outcome	Expected Value of Loss	%age of Overall Expected VOL	Class	Action	Total Cost	Minimize Expected Loss	Minimize Loss of Avail	Minimize Information Disclosure	Preserve Inforamation Integrity
PC1	Buffer Overflow	Information Integrity	$150,000	80%	B	Upgrade Software	$200	1	3	X	1
ES1	ICMP Implementation Malformed Path MTU DoS	Loss of Availability	$19,000	10%	C	Upgrade Software	$1,600	2	1	X	2
FW1	ICMP Implementation Malformed Path MTU DoS	Loss of Availability	$19,000	10%	C	Upgrade Software	$1,600	3	2	X	3

The personal computer in the network has the highest expected value of loss due to having a vulnerable version of Yahoo Messenger installed (SANS, 2005). The version of messenger installed on this system is susceptible to a buffer overflow attack. A buffer is a memory storage area that can overflow, if it is too small or the data being stored is inefficiently parsed. These overflows can be intentionally performed by attackers who use the overflow as a way to execute commands into other parts of the system, often resulting in information integrity issues (Merkow and Breithaupt, 2000). By addressing the buffer overflow vulnerability on the personal computer through upgrading the Yahoo Messenger application, the customer can decrease the expected value of loss by 80%, while only spending 13% of their $1500 budget. This upgrade is very inexpensive due to it being a simple task on a non-complex system and should only take an administrator a total of two hours.

The other two vulnerabilities are the "ICMP Implementation Malformed Path MTU DoS" (OSVDB, 2005) vulnerability, as already described in Section 6.4.3, affecting the manufacturer's

Cisco PIX 535 Firewall. In the customer system, the Cisco PIX 501 Firewall and the Windows 2003/Exchange Email Server are affected by this vulnerability. The fix for this vulnerability is a software upgrade as provided by the vendors. As discussed above, the cost of a software upgrade is estimated at $1600. This upgrade cost includes extensive testing and the backing up of files. Due to the relatively simple network and cost constraints, an abbreviated process for the upgrade might be considered by the customer in an attempt to stay within the budget.

6.5 Sensitivity Analysis

There are two areas of this risk assessment that required the introduction of subjective variables. In order to assess the validity of the values assigned to these variables, and the impact of those choices on the overall outcome of the analysis, a sensitivity analysis for each of those variables was performed. The sensitivity analysis was performed on the assigning of probabilities of a successful exploit of a vulnerability occurring and the assessment of outcomes stemming from an unauthorized result.

The method by which probabilities were determined and the way they are employed in this study might be better described as relative probabilities. By scoring characteristics of the vulnerability and then using that to determine the probabilities, the likelihood of a vulnerability occurring was given weighting relative to other vulnerabilities. The range of the possible probabilities used in the study was from 10% likelihood to 100% likelihood. By shrinking that range to 5% to 50% and then 50% to 100%, I found that the ranking of assets by expected value of loss was unchanged. By continuing to assume a linear relationship based on the scoring of the vulnerabilities as described, the probability assigned did adjusting the value of the expected value of loss, but it did not affect the expected value of loss ranking of assets. Performing this analysis

with a non-linear relationship between the score and probabilities assigned would also be interesting but has not been performed.

Changes in the outcomes have the most significant impact on the expected value of loss. The assignment of the outcomes to the three unauthorized results is another subjective portion of the analysis. For example, if the manufacturer were to decide that the nature of their business was such that in the event of a loss of availability instead of reclaiming 90% of the orders that were expected to be placed in the outage period, they only reclaimed 10%, this would increase the expected outcome by close to a factor of 10. At the same time, if the manufacturer decided that the impact on the long term commitment by the customer was only 1% of the customer base defecting due to an information integrity issue, rather than 10% that would reduce the expected value of loss by 80%. However, even these significant adjustments in the outcomes leave the rankings of projects based upon expected value of loss unchanged, as the impact of lost customers is so much greater than lost orders. Given the above, if the ranking of the projects were to be affected, the loss of availability would have to continue for 10 days in order for the value of the expected value of loss due to lost orders to exceed the expected value of loss for customer defection following information disclosure.

Despite the significant changes in the expected value of loss that can be achieved through changing the assumptions supporting the incident outcomes, the ranking of the projects is relatively stable. If the purpose of this assessment is to highlight areas of risk and indicate the priority of projects, there needs to be little concern over the exact calculation of the outcomes. If the outcomes are applied uniformly within the system, the criticality and priority as indicated by the relative expected value of loss should be consistent. The changes in outcomes will however, significantly change the dollar value of the risk per asset and overall system risk. If there is a

need for a high-level of accuracy in the expected value of loss for the purpose of considering insurance or reporting risk as part of a regulatory process, the investment of time for the appraisal of outcomes should be devoted accordingly.

7 Conclusions

The quantitative risk assessment methodology discussed in this paper is comprised by a series of phases including an asset inventory, vulnerability assessment, assignment of probabilities of unauthorized events and determination of consequences of unauthorized outcomes. Portions of this assessment are a fairly straightforward information gathering exercise, while other steps require the educated speculation based on an examination of the company and the business processes supported by the infrastructure and applications being assessed. Even the clearer cut information gathering stages have a time-sensitive nature that must be taken into account. Additionally, by understanding the areas within this assessment that are less straightforward and may require explanation and justification, a practitioner seeking to perform this type of assessment will be better prepared to both carry-out and then defend the results.

The asset inventory and the vulnerability assessment are the steps in the process that can be classified as clear information gathering. Both can be primarily performed with automated scanning, and while some analysis of vulnerabilities is recommended, the data gathered is relatively objective and can be counted on to be repeatable by others performing the same tests. The data that is generated gives a snap shot of the situation within the system at the time that the data gathering is completed.

The one area where this data can be questioned is its timeliness. The information security stance of a system is constantly changing. Assets are added and removed from the network and with

them the expected losses associated with the asset. Vulnerabilities are constantly being discovered, released to the public and then exploited. In order to be confident of the findings from the assessment, the data used as the base of this analysis should be regularly updated. By linking the outputs from automated scans to a database for this purposed, the task of continual updating could be made manageable.

There are other phases of the quantitative risk assessment that are subject to the discretion of the individuals performing the assessment. Assessing the outcomes of unauthorized results in the system is the most subjective process outlined in this study. The process for this phase as outlined in this methodology involves a discussion within the company to determine the possible outcomes by considering some quantifiable characteristics of the company such as size, business model, and number of customers, and then other non-quantifiable characteristics such as the type and strength of partner relationships. Once each of these characteristics of the business is determined, they are used as a basis for a subjective assessment of one of the main consequences considered, partner behavior. Predicting the response of customers to an information security breach at a particular company is highly subjective. If this process were to be more objective, the company being assessed would need historical data, which reflected the customer response to each unauthorized event, in order to better predict outcomes.

While changing the severity of the consequences associated with an unauthorized event can have a large impact on the expected values of losses and the ranking of projects, its subjective nature is defendable. The process of assigning the consequences by consulting the business makes it inherently reflect the tolerance within the business for unauthorized results. A perception by the business that a loss of availability would be crippling due to customer response to an outage will mean that vulnerabilities producing that result will be more heavily weighted. As long as the

same outcomes for a loss of availability are applied throughout the system, the risk analysis results will provide a consistent means by which to rank the mitigation projects.

The process required to perform a quantitative risk assessment of a system is not trivial. In a large system with hundreds of assets, the initial assessment could take months. Once the initial assessment is completed the changing nature of the security landscape could impinge the accuracy of the assessment almost immediately. However, with the aid of some automatic testing tools for both maintaining the asset inventory and vulnerability assessment, the quantitative risk assessment process is very useful in identifying critical areas of a system and prioritizing the work required to mitigate the risk.

8 Future Research

Quantitative risk assessments of systems' information security stance have not been widely researched. They are being carried out within companies, but there are some issues that hinder the assessment and cause the results to be questioned. The lack of historical data for determining the probabilities of incidents occurring and their outcomes makes the process of determining those values difficult and the results difficult to defend. The threat profile of a company can also evolve in a short period of time as a vulnerability progresses through the lifecycle of discovery to patch, with the status of the exploit changing throughout that time. Modeling that changing risk profile is a challenge.

One of the main issues with performing an information security quantitative risk assessment is that the lack historical data for determining probabilities of vulnerabilities being exploited and the outcomes resulting from a successful exploit. The relatively small number of incidents that occur within each company, and the hesitance of companies to report information security incidents have resulted in a lack of historical data regarding the consequences experienced by companies following a successful attack. Further efforts need to be made to develop historical data around information security incidents. Collecting data across organizations related to the probability of a vulnerability being exploited on a system would be very valuable. Additionally, further quantitative documentation of the outcomes following a successful exploit should be collected. By building historical stores of data regarding information security incidents, the need to use

subjective probabilities and develop subjective outcomes would be reduced, and the accuracy of risk assessments would be improved.

In order to be able to better model the stochastic nature of a vulnerability's lifecycle, further work should be done to develop a method for modeling the likelihood of different scenarios as a vulnerability's threat level evolves from release, through discovery of an exploit and the distribution of that exploit to the community. Developing such a model would provide the ability to look at the evolving threat profile of a vulnerability on an asset over a number of time periods to provide a better method for the prioritizing mitigation projects. Organizations are often limited in terms of the patching activities that they can perform by human resources. Modeling methods that support decision making for the development of ongoing mitigation plans are of great interests to many information security practitioners today.

Bibliography

Farahmand, F., Navathe, S., Sharp, G., and Enslow, P. (2003). Managing vulnerabilities of information systems to security incidents. ACM International Conference Proceeding Series, Proceedings of the 5th international conference on Electronic commerce. pp. 348-354.

Garg, A., Curtis, J., and Halper, H. (2003). Quantifying the financial impact of IT security breaches. Information Management and Computer Security. Vol.11 No. 2/3. pp. 74-83.

Getgen, K. (2005). Ten questions about Sarbanes-Oxley compliance. ComputerWorld, March 30, 2005.

Gordon, L. and Loeb, M. (2002). The Economies of Information Security Investment. ACM Transactions on Information and System Security. Vol 5. No. 4 (November), pp. 438-457.

Haimes, Y. Y. (1998). Risk Modeling, Assessment, and Management. John Wiley and Sons: New York.

Howard, J. D. and Longstaff, T.A. (1998) A Common Language for Computer Security Incidents. Sandia Report. SAND98-8667. October 1998. pp 1-26.

Huan, S, Sheoran, S, Wang, G. (2004) A review and analysis of supply chain operations reference (SCOR) model. Supply Chain Management. 2004. Vol. 9. Iss1. pp. 23-30.

ISO 7498-2:1989. (1989) Information processing systems: Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.

Kapuscinski, R., R. Zhang, P., Carbonneau, R., Moore, and B. Reeves, 2004, "Inventory Decisions in Dell's Supply Chain," Intervaces, v 34, no. 3 (May-June), pp191-205.

Lawrence, G., Loeb, M., Lucyshyn, W., and Richardson, R. (2004) CSI/FBI Computer Crime and Security Survey. Computer Security Institute Publication. 2004.

Lowrance, W.W. (1976) Of Acceptable Risk. William Kaufmann: Los Altos, CA.

Merkow, M. and Breithaupt, J. (2000). The Complete Guide to Internet Security. American Management Association: New York.

OSVDB. (2005). Open Source Vulnerability Database. Retrieved from www.osvdb.com.

SANS. (2005). "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus". Quarter 1 Update. SANS Institute. Retrieved from http://www.sans.org/top20/

Sarbanes Oxley Act of 2002. 15 USC.7201. (2002).

Scambray, J. and Shema M. (2002). Hacking Exposed Web Applications. New York: McGraw Hill/Osborne.

A Appendix A

Manufacturer Database Cost of Loss of Availability Calculation

Numbers highlighted in yellow are used in target calculation. Numbers highlighted in blue are the result of calculation

Length of Outage

1 day (Assumption of Assessment)

Number of Databases

2 databases (As per network design)

Revenue Transacted during Outage

Annual Revenue = $500,000,000

Number Trading Days Per Year = 251

Average Revenue Per Day = $500,000,000/251 = $1,992,000/Day

Percentage of Transactions Lost During Outage

10% (Outcome as Determined by Subjective Analysis)

Consequence of Loss of Availability to Database

Consequence = (10% * $1,992,000)/2 = $99,600

Manufacturer Database Cost of Loss of Information Integrity Calculation

Numbers highlighted in yellow are used in target calculation. Numbers highlighted in blue are the result of calculation

Cost of Customer Loss

Annual Revenue from Each Customer = Annual Revenue/Number of Customers
= $500,000,000/Year/500 customers = $1,000,000 Revenue/ Customer/Year

Percentage Customers Lost = 10% (Assumption of Assessment)

Number Customers Lost = 500 Customers * 10% = 50 Customers

Cost of Customers Lost Annually = 50 Customers*$1,000,000/Customer/ Year = $50,000,000/Year

Cost of Regulatory Fine

Regulatory Fine = $1,000,000 (Assumption of Assessment)

Cost of Labor to Restore Database

Average Hourly Rate for DBA = $150/Hour (Assumption of Assessment)

Number Hours to Restore Data = 160 Hours (Assumption of Assessment)

Cost of Labor = $150/Hour * 160 Hours = $24,000

Total Consequence of Loss of Information Integrity to Database

(Lost Customers+Regulatory+Labor)/Number of Databases =

($50,000,000+$1,000,000 + $24,000)/2= $25,512,000

Manufacturer Database Cost of Information Disclosure Calculation

Numbers highlighted in yellow are used in target calculation. Numbers highlighted in blue are the result of calculation

Consequence of Customer Loss

Annual Revenue from Each Customer = Annual Revenue/Number of Customers
= $500,000,000/Year/500 customers = $1,000,000 Revenue/ Customer/Year

Percentage Customers Lost = 5% (Assumption of Assessment)

Number Customers Lost = 500 Customers * 5% = 25 Customers

Cost of Customers Lost Annually = 50 Customers*$1,000,000/Customer/ Year = $25,000,000/Year

B Appendix B

Table 21 provides the list of vulnerabilities studied in this assessment and the corresponding URL's that provide descriptions of the vulnerabilities on the Open Source Vulnerabilities Database, SANS Top 20 List and Security Focus Website.

Table 21: Vulnerability Reference

Vulnerability Name	Vulnerability Description	Reference	Link to Reference
Cross Site Scripting	Malicious code inserted due to lack of validation parameters leading making it possible for user's to see each other's accounts.	Hacking Exposed	N/A
Apache 2 apr-util IPV6 Parsing DoS	IPv6 URI parsing routines in the apr-util library for Apache HTTP Server and IBM HTTP Server contains a flaw that may allow a remote denial of service	OSVDB/ID: 9994	http://www.osvdb.com/displayvuln.php?osvdb_id=9994
Sun Java System Web / Application Server Malformed Client Certificate DoS	The issue is triggered by the use of malformed client certificates, and will result in loss of availability for the server.	OSVDB/ID: 11383	http://www.osvdb.com/displayvuln.php?osvdb_id=11384
HTTP Server Format String	Check Point FireWall-1 HTTP Server Format String	OSVDB/ID: 4414	http://www.osvdb.com/displayvuln.php?osvdb_id=4414
D-Link Router DHCP Request Flood DoS	D-Link Router DHCP Request Flood DoS	OSVDB/ID: 7287	http://www.osvdb.com/displayvuln.php?osvdb_id=7287
SQL Injection	SQL Injection poosible in all application input fields	Hacking Exposed	N/A
ICMP Implementation Malformed Path MTU DoS	Triggered due to the handling of ICMP error messages and when the "Path MTU Discovery" (PMTUD) mechanism is used	OSVDB/ID: 15619	http://www.osvdb.com/displayvuln.php?osvdb_id=15619
Buffer Overflow	Old version of Yahoo Messenger	SANS 20 and Bugtraq/ID 9145	http://www.securityfocus.com/bid/9145 - http://www.sans.org/top20/#w10